

"Clean" Version of Added Claims

438. (New) An information management system comprising:
a plurality of workstations adapted for connection to a computer network, each workstation having a memory;
storage means for storing data received from each of said workstations;
application means, stored in said memory of each workstation, for transmitting outbound data to said network and receiving inbound data from said network;
policy storage means for providing policy data containing rules defining relevant data which is to be stored in said storage means; and
analyzing means, operable in conjunction with said policy means, for monitoring at least one of said outbound data and said inbound data, identifying in at least one of said outbound data and said inbound data, relevant data that is to be stored in said storage means in accordance with said rules in said policy means, and causing said relevant data to be stored in said storage means.
439. (New) The system of claim 438 wherein said relevant data that is to be stored in said storage means is encrypted prior to it being transmitted to said storage means.
440. (New) The system of claim 438 wherein said relevant data that is stored in said storage means is encrypted.
441. (New) The system of claim 438 wherein said computer network, to which said one or more workstations are adapted for connection, is the Internet.
442. (New) The system of claim 441 wherein said analyzing means is operable to identify, as relevant data, at least one of usernames and passwords used to identify a user, and usernames and passwords used to access web pages on the Internet, and the URL address of the web page at which those usernames and passwords are used,

said identified usernames, passwords and said identified URLs being stored in said storage means.

443. (New) The system of claim 442 wherein said analyzing means is operable to identify usernames and passwords from the field names of data contained in at least one of said outbound data and said inbound data.

444. (New) The system of claim 442 wherein a representation of the input fields of a web page is stored in said memory of said one or more workstations, and wherein said analyzing means is operable to identify usernames and passwords from said representation.

445. (New) The system of claim 442 wherein said analyzing means is operable to identify usernames or passwords from the field types of data contained in said outbound or said inbound data.

446. (New) The system of claim 441 wherein said analyzing means is operable to identify, as relevant data, digital certificates contained in at least one of said outbound or said inbound data or used to digitally sign signed data in said inbound data or said outbound data, or sufficient descriptive data to identify such digital certificates,
said digital certificates and/or said descriptive data being stored in said storage means.

447. (New) The system of claim 446 wherein said analyzing means is operable to identify one or more of the following data as relevant data:

- whether or not said digital certificate has been revoked;
- the identity of the holder of said digital certificate;
- the amount of any eCommerce transaction being made that is related to said digital certificate;

the goods or services being sold in any eCommerce transaction being made with said digital certificate;

the date of receipt of said digital certificate;

and wherein said identified data is stored with said digital certificate in said storage means.

448. (New) The system of claim 441 wherein the analyzing means is operable to identify when an eCommerce transaction is occurring and if an eCommerce transaction is identified as occurring, to identify in said outbound or said inbound data one or more of the following data as relevant data:

the URL address or e-mail address of the remote location to which outbound data is being transmitted or inbound data is being received;

the web pages accessed by a user of said one or more workstations during the transaction;

the amount of the transaction;

the goods or services being traded in the transaction;

the date of the transaction; and

wherein said relevant data is stored in said storage means.

449. (New) The system of claim 438 wherein said analyzing means is located on each of said one or more workstations.

450. (New) The system of claim 438 wherein said application means is a web browser.

451. (New) The system of claim 450 wherein said analyzing means is a plug-in module of said web browser.

452. (New) The system of claim 451 wherein said web browser is Microsoft's Internet Explorer and said analyzing means is a Browser Helper Object.

453. (New) The system of claim 438 wherein said application means is an e-mail client.

454. (New) The system of claim 453 wherein said analyzing means is a plug-in module of said e-mail client.

455. (New) The system of claim 454 wherein said e-mail client is Microsoft's Outlook e-mail client and said analyzing means is a Microsoft Exchange client extension.

456. (New) The system of claim 438 wherein said network includes a server and said analyzing means is located at a point on said network intermediate said one or more workstations and said server, or said analyzing means is located at said server.

457. (New) The system of claim 438 further comprising a supervisor workstation, said supervisor workstation having access to said storage means and being operable to view said relevant data stored in said storage means.

458. (New) The system of claim 457 wherein said policy storage means is accessible by said supervisor workstation, such that a user of said supervisor workstation can edit said policy data.

459. (New) The system of claim 438 wherein a workstation of said plurality of workstations has access to said storage means and is operable to view said relevant data stored in said storage means.

460. (New) The system of claim 438 wherein said computer network to which said one or more workstations are adapted for connection is a public computer network, and wherein said one or more workstations together form a private computer network.

461. (New) A system for recording passwords and usernames comprising:
a plurality of workstations adapted for connection to the Internet, each workstation having a memory;
storage means for receiving data from each of said workstations;
application means, stored in said memory of each workstation, for transmitting outbound data and receiving inbound data from the Internet; and/or application means for receiving user input data; and
analyzing means for monitoring at least one of said input data, said outbound data and said inbound data, to identify usernames and passwords contained in said user input data, said outbound data or said inbound data, and for causing said usernames and passwords to be stored in said storage means.

462. (New) The system of claim 461 wherein said analyzing means is operable to determine whether the usernames and passwords are used to access a web page, and if they are, to identify the URL address of said web page and cause said URL to be stored in said storage means with said usernames and passwords.

463. (New) The system of claim 461 wherein said relevant usernames and passwords data are encrypted prior to being transmitted to said storage means.

464. (New) The system of claim 461 wherein said relevant usernames and passwords that are stored in said storage means are encrypted.

465. (New) The system of claim 461 wherein said analyzing means is operable to identify said relevant usernames and passwords from the field names of data contained in at least one of said outbound data or said inbound data.

466. (New) The system of claim 461 wherein a representation of the input fields of a web page is stored in said memory of said one or more workstations, and wherein said

analyzing means is operable to identify said relevant usernames and passwords from said representation.

467. (New) The system of claim 461 wherein said analyzing means is operable to identify said relevant usernames or passwords from the field types of data contained in said outbound or said inbound data.

468. (New) The system of claim 461 wherein said application means has a user interface provided with a 'remember password' option which when selected stores input usernames and passwords in memory, and said analyzing means is operable to identify said relevant usernames and passwords in said input usernames and passwords stored in memory.

469. (New) The system of claim 461 wherein said analyzing means is located on each of said one or more workstations.

470. (New) The system of claim 461 wherein said application means is a web browser.

471. (New) The system of claim 470 wherein said analyzing means is a plug-in module of said web browser.

472. (New) The system of claim 471 wherein said web browser is Microsoft's Internet Explorer and said analyzing means is a Browser Helper Object.

473. (New) The system of claim 461 wherein said network comprises a server and said analyzer is located at a point on said network intermediate said one or more workstations and said server, or said analyzing means is located at said server.

474. (New) The system of claim 461 further comprising a supervisor workstation, said supervisor workstation having access to said storage means and being operable to view said relevant usernames and passwords stored in said storage means.

475. (New) The system of claim 461 wherein a workstation of said plurality of workstations has access to said storage means and is operable to view said relevant usernames and passwords stored in said storage means.

476. (New) An information management system comprising:

- one or more workstations adapted for connection to a computer network, each workstation having a memory;

- application means, stored in said memory of each workstation, for transmitting outbound data to said network and receiving inbound data from said network;

- policy storage means, for storing policy data containing rules specifying an appropriate encryption strength for outbound data, the encryption strength depending on the content of the data; and

- analyzing means, operable in conjunction with said policy data, for monitoring said outbound data to determine, in accordance with said rules in said policy data, an appropriate encryption strength for the outbound data;

- wherein said analyzing means controls transmission of said outbound data from said application means in dependence upon said determination of an appropriate encryption strength.

477. (New) The system of claim 476 wherein said rules in said policy data define confidential data which can not be transmitted, said analyzing means being operable in conjunction with said policy data to prevent said confidential data being transmitted from said application means.

478. (New) The system of claim 476 wherein said analyzing means is further operable to determine the present encryption strength in use for transmitting said outbound data; and

wherein said analyzing means controls transmission of said outbound data from said application means both in dependence upon said determination of an appropriate encryption strength and in dependence upon said determination of the present encryption strength in use.

479. (New) The system of claim 478 wherein if the analyzing means determines that the present encryption strength in use for transmitting outbound data is less than said appropriate encryption strength, then said analyzing means prevents transmission of said outbound data from said application means.

480. (New) The system of claim 478 wherein if the analyzing means determines that the present encryption strength in use for transmitting outbound data is less than said appropriate encryption strength, then said analyzing means prevents transmission of said outbound data from said application means and controls said application to renegotiate an encryption strength for transmission that is appropriate.

481. (New) The system of claim 478 wherein if the analyzing means determines that the present encryption strength in use for transmitting outbound data is less than said appropriate encryption strength, then said analyzing means modifies the outbound data such that the present encryption strength is an appropriate encryption strength for the transmission of the modified outbound data.

482. (New) The system of claim 478 wherein if the analyzing means determines that the present encryption strength in use for transmitting outbound data is less than said appropriate encryption strength, then said analyzing means controls said application means to notify a user of said application means that the encryption strength in use is not sufficient.

483. (New) The system of claim 476 wherein the analyzing means is further operable to identify credit card numbers in said outbound data.

484. (New) The system of claim 483 wherein the analyzing means is further operable to distinguish a predetermined set of credit card numbers from other credit card numbers, wherein said rules of said policy data define different appropriate encryption strengths for outbound data containing credit card numbers in the predetermined set than for other credit card numbers.

485. (New) The system of claim 484 wherein said rules of said policy data specify that there is no appropriate encryption strength for a pre-determined set of one or more credit card numbers.

486. (New) The system of claim 476 wherein said analyzing means is further operable to identify at least one or more of, credit card numbers, account codes, usernames, passwords, names and addresses and other predetermined keywords in the content of said outbound data.

487. (New) The system of claim 476 wherein said rules in said policy data specify an appropriate encryption strength for said outbound data, that is dependent on the address to which said outbound data is to be transmitted.

488. (New) The system of claim 476 wherein said analyzing means is located on each of said one or more workstations.

489. (New) The system of claim 476 wherein said application means is a web browser.

490. (New) The system of claim 489 wherein said analyzing means is a plug-in module of said web browser.
491. (New) The system of claim 490 wherein said web browser is Microsoft's Internet Explorer and said analyzing means is a Browser Helper Object.
492. (New) The system of claim 476 wherein said application means is an e-mail client.
493. (New) The system of claim 492 wherein said analyzing means is a plug-in module of said e-mail client.
494. (New) The system of claim 493 wherein said e-mail client is Microsoft's Outlook e-mail client and said analyzing means is a Microsoft client extension.
495. (New) The system of claim 476 wherein said network comprises a server and said analyzing means is located at a point on said network intermediate said one or more workstations and said server, or said analyzing means is located at said server.
496. (New) The system of claim 476 wherein said computer network to which said one or more workstations are adapted for connection is a public computer network, and wherein said one or more workstations together form a private computer network.
497. (New) The system of claim 476 further comprising a supervisor workstation, said policy data being accessible by said supervisor workstation, such that a user of said supervisor workstation can edit said policy data.
498. (New) An information management system comprising:
a plurality of client workstations adapted for connection to a computer network,
each workstation having a memory;

storage means for storing data received from each of said client workstations;
application means, stored in said memory of each workstation, for transmitting outbound data to said network and receiving inbound data from said network;

policy storage means for storing policy data defining rules for the recording of data that may comprise part of a transaction conducted between a client workstation and a third party across said computer network; and

analyzing means, operable in conjunction with said policy data, for analyzing at least one of said outbound data and said inbound data, to identify the existence of a transaction occurring between a client workstation and a third party, and for causing transaction data that is all or part of said outbound data or said inbound data related to an identified transaction to be stored in said storage means.

499. (New) The system of claim 498 wherein said analyzing means is operable to determine whether a secure link has been negotiated between said application means and a remote site on said network, and to identify the existence of a transaction if said outbound data or said inbound data is transmitted on a secure link.

500. (New) The system of claim 499 wherein said network is the Internet, and said rules of said policy data define the addresses of non-eCommerce web sites and/or non-eCommerce e-mail accounts, said analyzing means being operable to disregard any transactions that are identified between a client workstation and a non-eCommerce web site and/or e-mail account such that no transaction data related to a transaction made to a non-eCommerce web sites or a non-eCommerce e-mail account is stored in the storage means.

501. (New) The system of claim 498 wherein said analyzing means is operable to identify the existence of a transaction by reference to said rules of said policy data, said rules of said policy data defining the addresses of known eCommerce locations.

502. (New) The system of claim 498 wherein said analyzing means is operable to identify credit card numbers, and to identify the existence of a transaction by identifying credit card numbers in said outbound data or inbound data.

503. (New) The system of claim 498 wherein said analyzing means is operable to identify the existence of a transaction by reference to said rules of said policy data, said rules of said policy data defining one or more of pre-determined digital certificates, account codes, pre-determined keywords, pre-determined names and addresses and embedded codes.

504. (New) The system of claim 498 wherein said analyzing means is operable to identify embedded codes in said inbound data, said embedded code having been placed in said inbound data to identify it as transaction data.

505. (New) The system of claim 498 wherein said analyzing means is operable to identify electronic receipts, and to identify the existence of a transaction by identifying an electronic receipt in said outbound or inbound data.

506. (New) The system of claim 498 wherein said analyzing means is operable to record a pre-determined number of subsequent transmissions of said outbound data or said inbound data following an identification of the existence of a transaction by said analyzing means, providing that the address or organization to which the subsequent transmissions are sent, or from which they are received, is the same as the address or organization to which the outbound data was sent or from which the inbound data was received and in which the existence of a transaction was identified.

507. (New) The system of claim 506, wherein said analyzing means is operable to detect one or more indicators of the nature of the transaction, and said rules of said policy data define the number of subsequent transmissions of said outbound data and

said inbound data that are to be recorded in said storage means based on the identified nature of the transaction.

508. (New) The system of claim 506 wherein said rules of said policy data define the number of subsequent transmissions of said outbound and said inbound data that are to be stored in said storage means in dependence on the indicator by which the existence of a transaction was identified.

509. (New) The system of claim 498 wherein said analyzing means is operable to record all subsequent transmissions of said outbound data or said inbound data that occur within a pre-determined amount of time following an identification of the existence of a transaction by said analyzing means, providing that the address or organization to which the subsequent transmissions are sent, or from which they are received, is the same as the address or organization to which the outbound data was sent or from which the inbound data was received and in which the existence of a transaction was identified.

510. (New) The system of claim 509, wherein said analyzing means is operable to detect one or more indicators of the nature of the transaction, and said rules of said policy data define the amount of time for which all subsequent transmissions of said outbound data and said inbound data are to be recorded in said storage means based on the identified nature of the transaction.

511. (New) The system of claim 509 wherein said rules of said policy data define the amount of time for which subsequent transmissions of said outbound and said inbound data are to be stored in said storage means in dependence on the indicator by which the existence of a transaction was identified.

512. (New) The system of claim 498 wherein said analyzing means is further operable to identify the completion of a transaction by analyzing said outbound data or said

inbound data, and to cause all or part of said outbound data transmitted by said application means and all or part of said inbound data received by said application means after said analyzing means has identified the existence of a transaction and before said analyzing means has identified the completion of a transaction to be stored in said storage means.

513. (New) The system of claim 512 wherein said analyzing means is operable to identify subsequent related data in said outbound data transmitted by said application means and said inbound data received by said application means after said analyzing means has identified the completion of a transaction, and to cause said subsequent related data to be stored in said storage means with said transaction data already identified.

514. (New) The system of claim 513 wherein said analyzing means is operable to identify said subsequent related data by identifying common indicators in both said transaction data already identified and said outbound data transmitted by said application means and said inbound data received by said application means after said analyzing means has identified the completion of a transaction, said common indicators being one or more of the address of the location to which said outbound data is transmitted or from which said inbound data is received, part of the data path to the location to which said outbound data is transmitted or from which said inbound data is received, account code or reference numbers.

515. (New) The system of claim 498 wherein said application means is operable such that a user of said application means can indicate said outbound and said inbound data that is related to a transaction, said analyzing means being operable to identify said outbound and said inbound data so indicated.

516. (New) The system of claim 498 wherein said application means is operable to store all of said outbound data and said inbound data in said memory of said

workstation as previous data, irrespective of whether it may or may not be part of a transaction and, said analyzing means is operable, if the existence of a transaction is identified, to retrieve a pre-determined amount of previous data from said outbound data and said inbound data stored in said memory of said workstation, and to cause said previous data to be stored in said storage means with said transaction data.

517. (New) The system of claim 516 wherein said rules of said policy data specify the amount of previous data that is to be retrieved in dependence on the indicator by which the existence of a transaction is identified.

518. (New) The system of claim 516 wherein said network is the Internet and said application means is a web browser, said web browser being operable to store each web page that is viewed by said web browser in memory as previous data.

519. (New) The system of claim 518 wherein said rules of said policy data specify the number of web pages that are to be retrieved from those previously stored in memory in dependence on the indicator by which the existence of a transaction is identified.

520. (New) The system of claim 498 wherein said application means is operable to store all of said outbound data and said inbound data in memory as previous data, irrespective of whether it may or may not be part of a transaction and, said analyzing means is operable, if the existence of a transaction is identified, to identify, in said previous data, earlier relevant data that is related to said transaction data already identified, and to cause said earlier relevant data to be stored in said storage means with said transaction data.

521. (New) The system of claim 520 wherein said analyzing means is operable to identify said earlier relevant data in said previous data, by identifying common indicators in both said transaction data and said outbound data and said inbound data previously stored in said memory of said workstation, said common indicators being

one or more of the address of the location to which said outbound data is transmitted or from which said inbound data is received, part of the data path to the location to which said outbound data is transmitted or said inbound data is received, account code or reference number.

522. (New) The system of claim 498 wherein said application means is operable to store all of said outbound data and said inbound data in memory as previous data, irrespective of whether it may or may not be part of a transaction, and is further operable such that, if said analyzing means identifies the existence of a transaction, a user of said application means can select earlier relevant data from said previous data, said earlier relevant data selected by the user being stored in said common storage means together with said transaction data.

523. (New) The system of claim 498 wherein said analyzing means is operable, once it has identified the existence of a transaction, to determine the nature of said transaction by analyzing the content of said outbound and inbound data, and said rules of said policy data define how said transaction data is to be stored in said storage means in dependence on the nature of the transaction determined by said analyzing means, said transaction data being stored in said database according to said determination and said rules of said policy data.

524. (New) The system of claim 523 wherein said analyzing means is operable to determine the nature of the transaction by identifying in said outbound data and said inbound data one or more indicators, said indicators being defined in said rules of said policy data, and being one or more of: the address of the network location to which said data that may be part of a transaction is transmitted or from which it is received; part of the data path to the network location to which said transaction data is transmitted or from which it is received; account codes; reference numbers; credit card numbers; digital certificates and pre-determined keywords.

525. (New) The system of claim 498 wherein said analyzing means is operable to identify, once the existence of a transaction has been identified, one or more indicators of the nature of said transaction, said transaction data being stored in said storage means such that it is organized by said one or more indicators to form a record.

526. (New) The system of claim 525 wherein said rules of said policy data define said one or more indicators of the nature of a transaction, said indicators being one or more of: the address of the location to which said transaction data is transmitted or from which it is received; part of the data path to the location to which said transaction data is transmitted or from which it is received; account codes, reference numbers, credit card numbers, digital certificates and pre-determined keywords.

527. (New) The system of claim 498 wherein said storage means is accessible by one or more of an accounts application, an order processing application or other transaction management application.

528. (New) The system of claim 498 wherein any data transmitted to said storage means is encrypted before it is transmitted to said storage means.

529. (New) The system of claim 498 wherein any data stored in said storage means is encrypted.

530. (New) The system of claim 498 wherein said analyzing means is located on each of said one or more workstations.

531. (New) The system of claim 498 wherein said application is a web browser.

532. (New) The system of claim 531 wherein said analyzing means is a plug-in module of said web browser.

533. (New) The system of claim 532 wherein said web browser is Microsoft's Internet Explorer and said analyzing means is a Browser Helper Object.

534. (New) The system of claim 498 wherein said application means is an e-mail client.

535. (New) The system of claim 534 wherein said analyzing means is a plug-in module of said e-mail client.

536. (New) The system of claim 535 wherein said e-mail client is Microsoft's Outlook e-mail client and said analyzing means is a Microsoft Exchange client extension.

537. (New) The system of claim 498 wherein said network comprises a server, and said analyzing means is located at a point on said network intermediate said one or more work stations and said server, or said analyzing means is located at said server.

538. (New) The system of claim 498 wherein said computer network to which said one or more workstations are adapted for connection is a public computer network, and wherein said one or more workstations together form a private computer network.

539. (New) The system of claim 498 further comprising a supervisor workstation, said policy data being accessible by said supervisor workstation, such that a user of said supervisor workstation can edit said policy data.

540. (New) An information management system comprising:

one or more workstations adapted for connection to a computer network, each workstation having a memory;

application means, stored in said memory of each workstation, for transmitting outbound data to said network and receiving inbound data from said network;

policy storage means for storing policy data, containing rules for the transmission of outbound data that may be part of a transaction; and

analyzer means, operable in conjunction with said policy data, for identifying in at least said outbound data, transaction data that may be part of a transaction, and for determining, in accordance with said rules of said policy data, whether the transmission of said transaction data would satisfy said rules;

and wherein the transmission of said transaction data by said application means is dependent on said determination made by said analyzing means.

541. (New) The system of claim 540, wherein according to said determination made by said analyzing means, said transaction data is either, transmitted, not transmitted, or sent to an approver who determines whether or not to transmit the transaction data.

542. (New) The system of claim 541 further comprising:

one or more approvers, for deciding whether the transmission of said data that may be part of a transaction may be made;

wherein said analyzing means is operable to identify in said data that may be part of a transaction, data that needs approval and to refer said data that needs approval to one of said one or more approvers; and

the transmission of said data that needs approval being dependent on the decision of said one or more approver.

543. (New) The system of claim 542 wherein said analyzing means is operable to identify said transaction data that needs approval by determining the nature of said transaction data and by checking said rules of said policy data, said rules of said policy data defining whether or not approval is needed in dependence on the determined nature of said transaction data.

544. (New) The system of claim 542 wherein said analyzing means is operable to determine the nature of said transaction data by identifying at least one of the identity

of the transmitter of said data, the identity of the intended recipient of said data, the workstation from which said data is to be transmitted, the sum for which a transaction is to be made, and the account against which a transaction is to be made.

545. (New) The system of claim 542 wherein said analyzing means is operable to determine the nature of said transaction data that needs approval and to select said one of said one or more approvers in dependence on that determination.

546. (New) The system of claim 545 wherein said analyzing means is operable to determine the nature of said transaction data that needs approval by identifying at least one of the identity of the transmitter of said data, the identity of the intended recipient of said data, the work station from which said data is to be transmitted, the sum for which a transaction is to be made, and the account against which the transaction is to be made.

547. (New) The system of claim 540 wherein said analyzing means is operable to determine whether a secure link has been negotiated between said application and a remote site on said network, and to identify said outbound data or said inbound data as transaction data, if it is transmitted on a secure link.

548. (New) The system of claim 547 wherein said network is the Internet, and said rules of said policy data define the addresses of web sites or e-mail accounts that negotiate secure links for the transmission of data but which are known not to be eCommerce sites or accounts, said analyzing means being operable to disregard said outbound data transmitted to those web sites or accounts or said inbound data received from those web sites or accounts, such that no approval is required.

549. (New) The system of claim 540 wherein said analyzing means is operable to identify transaction data by reference to said rules of said policy data, said rules of said policy data defining the addresses of known eCommerce web sites and e-mail accounts.

550. (New) The system of claim 540 wherein said analyzing means is operable to identify credit card numbers in said outbound data or said inbound data, and to identify outbound data or inbound data that contains a credit card number as transaction data.

551. (New) The system of claim 550 wherein said policy data specifies pre-determined credit card numbers that can never be transmitted.

552. (New) The system of claim 540 wherein said analyzing means is operable to identify transaction data by reference to said rules of said policy data, said rules of said policy data defining one or more of pre-determined digital certificates, account codes, pre-determined keywords, pre-determined names and addresses and embedded codes.

553. (New) The system of claim 540 wherein said analyzing means is operable to identify embedded codes in said inbound data, said embedded codes having been placed in said inbound data to mark said inbound data as transaction data.

554. (New) The system of claim 540 wherein said application is operable such that a user of said application can indicate said outbound and said inbound data that is part of a transaction, said analyzing means being operable to identify said outbound and said inbound data so indicated.

555. (New) The system of claim 540 wherein said analyzing means is located on each of said one or more workstations.

556. (New) The system of claim 540 wherein said application is a web browser.

557. (New) The system of claim 556 wherein said analyzing means is a plug-in module of said web browser.

558. (New) The system of claim 557 wherein said web browser is Microsoft's Internet Explorer and said analyzing means is a Browser Helper Object.

559. (New) The system of claim 540 wherein said application is an e-mail client.

560. (New) The system of claim 559 wherein said analyzing means is a plug-in module of said e-mail client.

561. (New) The system of claim 560 wherein said e-mail client is Microsoft's Outlook e-mail client and said analyzing means is a Microsoft Exchange client extension.

562. (New) The system of claim 540 wherein said network comprises a server and said analyzing means is located at a point on said network intermediate said one or more workstations and said server, or said analyzing means is located at said server.

563. (New) The system of claim 540 wherein said computer network to which said one or more workstations are adapted for connection is a public computer network, and wherein said one or more workstations together form a private computer network.

564. (New) The system of claim 540 further comprising a supervisor workstation, said policy data being accessible by said supervisor workstation, such that a user of said supervisor workstation can edit said policy data.

565. (New) An information management system comprising:
one or more workstations adapted for connection to a computer network, each workstation having a memory;
application means, stored in said memory of each workstation, for receiving at least inbound data from said network;

analyzing means, being operable in conjunction with said application means, for monitoring said inbound data to identify in at least said inbound data signed data that has been digitally signed with a digital certificate, for extracting one or more details of said signed data and for determining whether or not verification is required for said digital certificate;

policy storage means, accessible by said analyzing means, for storing policy data containing rules which define whether or not verification is required for said digital certificate;

and wherein said analyzing means determines whether or not verification is required for said digital certificate in dependence on said rules of said policy data and in dependence on said one or more details of said signed data extracted by said analyzing means.

566. (New) The system of claim 565 wherein said verification for said digital certificate includes determining whether said digital certificate has been revoked.

567. (New) The system of claim 566 wherein said analyzing means is further operable to determine whether said signed data is part of an eCommerce transaction, and if it is, to determine the amount of money that is promised in that eCommerce transaction, wherein said verification for the digital certificate also includes determining whether said digital certificate can be taken as a guarantee of receiving the amount of money promised in said eCommerce transaction.

568. (New) The system of claim 565 wherein said analyzing means is operable to extract as one or more details of said signed data, one or more of said digital certificate holder's identity, the expiry date of said digital certificate, the issue number of said digital certificate, and the domain name from which the signed data was received, and wherein said rules of said policy file define whether or not verification for said digital certificate is required in dependence on the one or more details extracted by said analyzing means.

569. (New) The system of claim 565 wherein said analyzing means is operable to determine whether or not an eCommerce transaction is occurring, and to extract, as one or more details of said signed data, the amount of any transaction being made with said digital certificate, the account code from which any payment is being made, a credit card number, one or more indicators of the nature of the transaction, and wherein said rules of said policy file define whether or not verification is required for a digital certificate in dependence on the one or more details extracted by said analyzing means.

570. (New) The system of claim 569 further comprising a data repository in which, digital certificates used to digitally sign any previously received signed data or sufficient descriptive data to identify any such digital certificates, and transaction data describing any previous transactions made with those digital certificates are stored,
said transaction data being at least one or more of the date of any previous transactions made with a digital certificate, and the amount of any previous transaction made with that digital certificate,
and wherein said rules of said policy file define whether or not verification for said digital certificate is required in dependence on said transaction data.

571. (New) The system of claim 565 further comprising a data repository, accessible by said analyzing means, wherein said analyzing means is operable to identify any digital certificates that are used to digitally sign signed data in at least said inbound data, and to cause any such digital certificates, or sufficient descriptive data to identify such digital certificates to be stored in said data repository.

572. (New) The system of claim 571 wherein said analyzing means is operable, to record the results of any verification for an digital certificate in said data repository together with said digital certificate or together with said descriptive data.

573. (New) The system of claim 572 wherein said analyzing means is operable, if it identifies a digital certificate in said inbound data, to determine whether said digital certificate has been previously stored in said data repository, or whether said descriptive information identifying said digital certificate has been stored in said data repository, and if said digital certificate has been previously stored, to look-up the results of any previous verification of whether said digital certificate has been revoked, wherein said analyzing means determines whether or not to verify if said digital certificate has been revoked in dependence on said results of any previous verification of whether said identified digital certificate has been revoked.

574. (New) The system of claim 565 wherein said analyzing means is further operable to verify whether or not a digital certificate has been revoked, and wherein said application means is operable to prevent said inbound data being viewed by a user of said application means if said analyzing means determines that said digital certificate has been revoked.

575. (New) The system of claim 565 wherein said analyzing means is further operable to verify whether or not a digital certificate has been revoked, and said application means is operable to notify a user of said application means that said inbound data is not to be relied upon if said analyzing means determines that said digital certificate has been revoked.

576. (New) The system of claim 565 wherein said analyzing means is located on each of said one or more workstations.

577. (New) The system of claim 565 wherein said application means is a web browser.

578. (New) The system of claim 577 wherein said analyzing means is a plug-in module of said web browser.

579. (New) The system of claim 578 wherein said web browser is Microsoft's Internet Explorer and said analyzing means is a Browser Helper Object.

580. (New) The system of claim 565 wherein said application means is an e-mail client.

581. (New) The system of claim 580 wherein said analyzing means is a plug-in module of said e-mail client.

582. (New) The system of claim 581 wherein said e-mail client is Microsoft's Outlook e-mail client and said analyzing means is a Microsoft client extension.

583. (New) The system of claim 565 wherein said network comprises a server, and said analyzing means is located at a point on said network intermediate said one or more workstations and said server, or said analyzing means is located at said server.

584. (New) The system of claim 565 wherein said computer network to which said one or more workstations are adapted for connection is a public computer network, and wherein said one or more workstations together form a private computer network.

585. (New) The system of claim 565 further comprising a supervisor workstation, said policy data being accessible by said supervisor workstation, such that a user of said supervisor workstation can edit said policy data.